(19)日本国特許庁（ＪＰ）　(12) 公表特許公報（Ａ）　(11)特許出願公表番号

特表平8－506217

(43)公表日　平成８年(1996)７月２日

(51)Int.Cl.⁶		識別記号	庁内整理番号	ＦＩ
Ｈ０４Ｌ	9/00			
Ｇ０９Ｃ	1/00		7259－5Ｊ	
Ｈ０４Ｌ	9/10			
	9/12			
			8842－5Ｊ	Ｈ０４Ｌ　9／00　Ｚ

審査請求　未請求　予備審査請求　有　（全 28 頁）

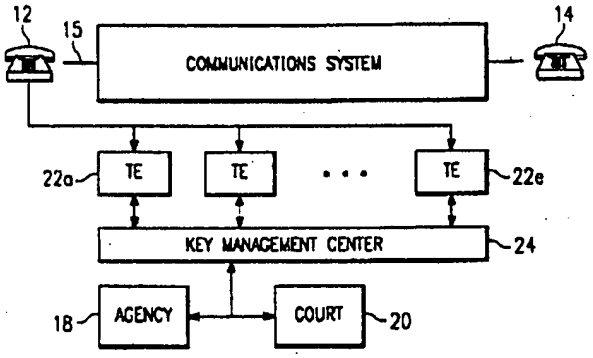
(21)出願番号　特願平5－518661
(86)（22)出願日　平成５年(1993)４月20日
(85)翻訳文提出日　平成６年(1994)10月20日
(86)国際出願番号　ＰＣＴ／ＵＳ９３／０３６６６
(87)国際公開番号　ＷＯ９３／２１７０８
(87)国際公開日　平成５年(1993)10月28日
(81)指定国　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＤＥ，ＤＫ，ＥＳ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＡＵ，ＣＡ，ＪＰ，ＫＲ

(71)出願人　ミカリ，シルヴィオ
アメリカ合衆国マサチューシッツ州02146、ブルックライン、チェスナット・ヒル・アヴィニュー　459番
(72)発明者　ミカリ，シルヴィオ
アメリカ合衆国マサチューシッツ州02140、ケイムブリッジ、アプランド・ロウド　224番
(74)代理人　弁理士　真田　雄造　（外１名）

(54)【発明の名称】　公正な暗号システム及びその使用方法

(57)【要約】
各ユーザーには突き合せたシクレットキーとパブリックキーの一対が割当てられている、適法のユーザーのプライバシーを保護しながら不法な活動の疑いのあるユーザーの通信を予め定められたエンティティ（18）が監視できるようにするためのパブリックキー暗号システムを用いた方法。この方法に従うと各ユーザーのシクレットキーは、分担分に分割される。次に各ユーザーは、複数の「受託者」（22a）に情報断片を提供する。各受託者（22a）に提供された情報断片は、このような情報がいくつかの与えられたパブリックキーの１シクレットキーの１「分担分」を含んでいることをその受託者（22a）が確認できるようにする。各各の受託者（22a）は、他のいずれの受託者（22a）とも対話することなく、又はユーザーにメッセージを送ることによつて、提供された情報断片がシクレットキーの分担分を含んでいることを確認できる。予め定められた要請または条件、例えば不法な活動の疑いのあるユーザーの通信を監視することをエンティティ（18）に許可する裁判所命令（20）などに基づいて、受託者（22a）はエンティティ（18）に対しこの

FIG. 2



【特許請求の範囲】

1． 遵法のユーザーのプライバシーを保護しながら不法な活動の疑いのあるユーザーの通信を予め定められたエンティティーが監視できるようにするためのパブリックキー暗号システムを用いた方法において、各各のユーザーには突き合わせたシクレットキーとパブリックキーの対が割当てられている方法において、

各ユーザーのシクレットキーを分担分に分割する段階と、

情報断片にいくつかの与えられたパブリックキーの１つのシクレットキーの分担分が含まれていることを受託者が検証できるようにする情報断片を受託者に提供する段階と、

予め定められた要請に基づいて、不法活動の疑義あるユーザーに対する通信を監視するために、シクレットキーの再構成をエンティティが試みることができるようにするため、被疑者であるユーザーのシクレットキーの分担分を受託者に暴露させる段階と、

を含む方法。

2． 予め定められたエンティティーが政府機関であり、予め定められた要請が裁判所命令である、請求の範囲第１項に記載の方法。

3． 被疑者ユーザーのアイデンティティが受託者に認知されている、請求の範囲第１項に記載の方法。

4． 被疑者ユーザーのアイデンティティが受託者にとつて未知のものである、請求の範囲第１項に記載の方法。

5． エンティティが被疑者ユーザーの通信を監視できない場合、被疑者ユーザーの活動を不法なものとして特徴づけする段階、

をさらに含む、請求の範囲第１項に記載の方法。

6． シクレットキーを再構成するためには、被疑者ユーザーのシクレットキーの分担分の全てではなくそれより少ないものの暴露しか必要とされない、請求の範囲第１項に記載の方法。

7． 予め定められた要請に基づいて分担分がエンティティに対し暴露される、請求の範囲第１項に記載の方法。

8．　一定の与えられた少数の受託者にはシクレットキーを再構成できない、請求の範囲第１項に記載の方法。

9．　各各の受託者が、他のいずれの受託者との対話もなしに、提供された情報断片がシクレットキーの１分担分を含んでいることを確認できる、請求の範囲第１項に

記載の方法。

10．　遵法のユーザーのプライバシーを保護しながら不法な活動の疑いのあるユーザーの通信を予め定められたエンティティが監視できるようにするための、暗号システム内へのパブリックキー暗号システムを使用する方法において、

各各の受託者が、受理した分担分がいずれかのパブリックキーのシクレットキーの一部であることを確認できるように、複数の受託者と各ユーザーのシクレットキーを検証可能な形で秘密共有する段階、

を含む方法。

11．　遵法のユーザーのプライバシーを保護しながら不法な活動の疑いのあるユーザーの通信を予め定められたエンティティが監視できるようにするための、パブリックキー暗号システムを用いた方法において、各ユーザーには符合するシクレットキーとパブリックキーの一対が割当てられる方法において、

各ユーザーのシクレットキーを分担分に分割する段階と、

いくつかの与えられたパブリックキーの１つのシクレットキーの分担分を含む情報断片を受託者に提供する段階と、

予め定められた要請に基づいて、エンティティがシク

レットキーを再構成し被疑者ユーザーに対する通信を監視することができるようにするための不法な活動の疑いのあるユーザーのシクレットキーの分担分を受託者に暴露させる段階、

を含む方法。

12．　エンティティが被疑者ユーザーの通信を監視できない場合、被疑者ユーザーの活動を不法なものとして特徴づけする段階、

をさらに含む、請求の範囲第１０項に記載の方法。

13. 一定の与えられた少数の受託者にはシクレットキーを再構成できない、請求の範囲第１０項に記載の方法。

14. 各受託者は、その他のいずれの受託者とも対話することなく、提供された情報断片がシクレットキーの分担分を含んでいることを確認することができる、請求の範囲第１０項に記載の方法。

15. 遵法のユーザーのプライバシーを保護しながら不法な活動の疑いのあるユーザーの通信を予め定められたエンティティが監視できるようにするための、暗号システムを使用し、かつ一群のユーザーに１つのシクレットキーを持たせる方法において、

シクレットキーを分担分に分割する段階と、

シクレットキーの分担分を含む情報断片を受託者に提供する段階と、

予め定められた要請に基づいて、エンティティがシクレットキーを再構成し被疑者ユーザーに対する通信を監視することができるようにするための不法な活動の疑いのあるユーザーのシクレットキーの分担分を受託人に暴露させる段階と、

を含む方法。

16. エンティティが被疑者ユーザーの通信を監視できない場合、被疑者ユーザーの活動を不法なものとして特徴づけする段階、

をさらに含む、請求の範囲第１５項に記載の方法。

17. 一定の与えられた少数の受託者にはシクレットキーを再構成できない、請求の範囲第１５項に記載の方法。

18. 各受託者は、その他のいずれの受託者とも対話することなく、提供された情報断片がシクレットキーの分担分を含んでいることを検証することができる、請求の範囲第１５項に記載の方法。

【発明の詳細な説明】

名称　　公正な暗号システム及びその使用方法

技術分野

本発明は、一般に秘密システム（ｃｒｙｐｔｏｓｙｓｔｅｍ）［以下暗システムと呼ぶ］より特定的には、遵法のユーザーのプライバシーを保護しながら不法な活動の疑いのあるユーザーの通信を一定の与えられた統一体が監視できるようにするための方法に関する。

背景技術

シングルキー暗号システムにおいては、共通の１つのシクレットキー（ｓｅｃｒｅｔ　ｋｅｙ）がメッセージの暗号化（ｅｎｃｒｙｐｔｉｎｇ）或いは解説（ｄｅｃｒｙｐｔｉｎｇ）のいずれにも利用される。かくして、このようなキーを予め安全に交換した２人の加入者のみがこれらのシステムを秘密通信のために使用できる。このことは、シングルキーシステムの利用可能性を著しく制限している。

ダブルキー暗号システムにおいては、暗号化及び解読のプロセスが異なるキーにより支配される点が異なっている。基本的に、突き合わせた（ｍａｔｃｈｉｎｇ）暗号化及び暗号解読キーの一対が考え出される。一定の与えられた暗号化キーを用いて暗号化されるものは、対応する暗号解読キーを用いてはじめて解読できる。その上、

暗号化キーはそれに突き合せた解読キーを「密告」しない。すなわち、暗号化キーを知っていることが暗号解読キーの値を見い出す助けとはならない。ダブルキーシステムの利点は、いかなるキーも安全に交換したことのない２人の加入者が非機密保持通信回線（すなわち敵により傍受される可能性のある通信回線）上で秘密に通信することを可能にすることができるということにある。彼らは、オンライン専用通信プロトコルを実行することによつてこれを行なう。

特に、加入者Ａは加入者Ｂに対し、自らが内密に話したいことがあるという警告を発する。すると加入者Ｂは、一対の符合する暗号化及び暗号解読キー（E_B，D_B）を計算する。次にＢはＡにキーE_Bを送る。加入者Ａはこのとき自らのメ

ッセージmを暗号化し、暗号文ｃ＝E_B（m）を得、非機密保持通信回線上でｃをＢに送る。Ｂは、m＝D_B（ｃ）を計算することにより暗号文を解読する。敵がＡとＢの間の全ての通信を盗聴する場合、この敵はＢの暗号化キーE_BとＡの暗号文ｃの両方を開くことになる。しかしながら、敵はＢの解読キーD_Bを知らないためｃからmを計算できない。

上述のプロトコルのもつ利点は、次の２つの欠点にさいなまれていることから、なお極めて限られたものとなとている。まず第１にＡがＢに秘密メッセージを送るためには、少なくとも初回はＢからＡにメッセージを送ることも必要であるという点である。いくつかの状況の下

では、このことは全くの欠点である。さらにＡは、（いずれにせよ通信回線は機密保持されていないのであるから）、受理したストリングD_Bが実際にＢの暗号化キーであるという保証をもたない。実際、これは敵によつて送られたキーである可能性もあり、こうして敵はそれに続く暗号化された伝送を理解することになる。

普通のパブリックキー（ｐｕｂｌｉｃ　ｋｅｙ）暗号システム（「ＰＫＣ」）が両方の問題点を解決し、通信を大幅に容易にする。このようなシステムは基本的に、適切なキー管理センターと共にダブルキーシステムを使用することから成る。各各のユーザーｘは、ダブルキーシステムの一対の符号する暗号化及び暗号解読キー（Ｅｘ，Ｄｘ）を考え出す。彼は、自らのためにＤｘをとっておき、Ｅｘをキー管理センターに与える。センターは、各ユーザーについての正しいパブリックキーのダイレクトリすなわちタイプ（Ｘ，Ｅｘ）の入力の正しいリストを更新し公表する責任をもつ。例えば、ｘから自らのパブリックキーとしてＥｘを有するよう要請を受けた時点て、センターはｘのアイデンティティを適切にチェックし、全ての暗号化キーに有効期限がある場合には現日付と共に対（Ｘ，Ｅｘ）に（デジタル式に）署名する。センターは、署名された情報をシステム内の全てのユーザーに分配することによりＥｘを公表する。このようにして、いかなる対話もなしに、ユーザーは、センターが公表するダイレクトリの中で照合できる自らのパブリック

暗号化キーを介して秘密メッセージを互いに送ることができる。センターが対（Ｘ，Ｅｘ）に署名しているということは、その対がすでに検査済みのＸのアイデンティティを有するセンターにより分配されたものである、ということを保証しているため、アイデンティティの問題も又解決される。

ＰＫＣの便宜性はキー管理センターに依存している。大規模にこのようなセンターを創設するには多大な努力が必要であるため、追従すべき明確なプロトコルを適切に選ばなくてはならない。さらに、パブリックキー暗号にはいくつかの欠点がある。主たる欠点は、かかるシステムの全てが例えば、（当局の知らないうちに）独自のＰＫＣを使用しかくして自らの不法な取引を極秘裏にしかも極めて便利に行うことのできる犯罪組織やテロリストによつて濫用されうる、ということにある。

従って、その正当な利点の全てを維持しながらパブリックキー暗号システムのあらゆる濫用を防ぐことが望ましい。

本発明の目的は、同時に遵法のユーザーのプライバシーを保護しながら不法な活動の疑いのあるユーザーの通信を、政府といつた一定の与えられたエンティティ（ｅｎｔｉｔｙ）が監視できるようにするための方法を提供することにある。

本発明のさらにもう１つの目的は、パブリックキー又はプライベートキーの暗号システムのいずれかを用いた

このような方法を提供することにある。

本発明のさらにもう１つの目的は、予め定められたできごと例えば裁判所命令の取得があつた時点ではじめて被疑者ユーザーの通信をエンティティが監視できる、いわゆる「公正な」暗号システムを提供することにある。

もう１つの目的は、このような通信技術において使用するための公正な暗号システムを構築する方法を記述することにある。

１実施態様においては、本発明のこれらの及びその他の目的は、各ユーザーに対し一対の符合するシクレット及びパブリックキーが割当てられている、遵法のユーザーのプライバシーを保護しながら不法な活動の疑いのあるユーザーの通信を予め定められたエンティティが監視できるようにするための、パブリックキー

暗号システムを用いた１つの方法の中で提供されている。この方法に従うと、各ユーザーのシクレットキーは、分担分（ｓｈａｒｅｓ）へと分割される。次に各ユーザーは複数の「受託者」（ｔｒｕｓｔｅｅｓ）に情報断片を提供する。各受託者に提供された情報断片により、その受託者は、かかる情報に一定の与えられたパブリックキーのクレジットキーの１「分担分」が含まれていることを確認することができる。さらに、各受託者は、その他のいずれの受託者とも対話することなく、又はユーザーにメッセージを送ることにより、提供された情報断片がシクレットキーの１分担分を含んでいることを確認することができ

る。予め定められた要請又は条件、例えば、不法な活動の疑いのあるユーザーの通信を監視することをエンティティに許可する裁判所命令に基づいて、受託者は、エンティティがシクレットキーを再構成し被疑者ユーザーの通信を監視できるようにするため、このようなユーザーのシクレットキーの分担分を統一体に暴露する。

この方法は、受託者が被疑者ユーザーのアイデンティティを知っているか否かに関わらず実施でき、又シクレットキーを再構成するために被疑者ユーザーのシクレットキーの分担分の全てではなくそれより少ない部分の暴露しか必要とされない場合でさえ、実施できる。この方法は充分頑強なものであるため一定の与えられた少数の受託者が疑惑の目にさらされエンティティに協力するべく信頼され得ない場合にも有効である。さらに、被疑人ユーザーの活動は、統一体がシクレットキーを再構成した後又はこれを再構成しようと試みた後でも被疑者ユーザーの通信を監視できない場合、不法なものとして特徴づけされる。

本発明のもう一つのより一般化された態様に従うと、遵法のユーザーのプライバシーを保護しながら不法な活動の疑いのあるユーザーの通信を定められたエンティティが監視できるようにするためにパブリックキー暗号システムを用いるための方法が記述されている。この方法には、各各の受託者が、受理した分担分が或るパブリックキーの１シクレットキーの一部であることを確認でき

るように、各各のユーザーのシクレットキーを複数の受託者と「確認可能な形で

秘密共有する」段階が含まれている。

以上で、本発明のより適切な目的のいくつかを概略的に記した。これらの目的は、本発明のより卓越した特徴及び応用のいくつかを例示するにすぎないものとみなされるべきである。開示した発明を異なる要領で応用するか又は以下で記述するように本発明を修正することにより、その他の有益な結果が数多く達成できる。従って、好ましい実施態様について以下の詳細な説明を参照することにより、本発明のその他の目的及びより完全な理解を得ることができるだろう。

本発明及びその利点をより完璧に理解するには、以下の添付図面に結びつけて以下の詳細な説明を参照するべきである。なお図面中、図１は、政府エンティティ（ｇｏｖｅｒｎｍｅｎｔ　ｅｎｔｉｔｙ）が、不法な活動の疑いのあるユーザーの通信を監視することを望む通信システムの簡略化された図である。

図２は、不法な活動の疑いのあるユーザーの通信を監視するため本発明の方法を使用できるエンティティの好ましい階層のブロックダイヤグラムである。

図１は、発呼局１２と被呼局１４の間に接続された電話回線網を含む単純な通信システム１０を表わしている。単数又は複数の地方電話交換局又は電話スイッチ１６が、周知の方法で回線網全体にわたり電話信号を接続してい

る。ここで図２も参照してみると、地方の法執行機関１８といつた政府エンティティが、発呼局のユーザーに不法な活動の疑いがあることを理由としてこの発呼局１２へ及び／又はこの発呼局からの通信を監視することを望んでいる、と仮定しよう。さらに、発呼局１２のユーザーがＰＫＣを用いて通信しているということも仮定する。受入れられている合法的実践法に従って、政府機関１８は、この回線１５をひそかに監視するべく裁判所２０から裁判所命令を得る。本発明に従うと、政府機関は、回線網内のその他の遵法のユーザーのプライバシー権を同時に維持しながら、回線１５を監視することができる。これは、以下で記述するようにね各各のユーザーが複数の受託者２２ａ･･･２２ｎとユーザーシクレットキー（ＰＫＣの）を「秘密共有」することを要求することによつて達成される。

本発明に従うと、「公正な」ＰＫＣは、特殊なタイプのパブリックキー暗号システムである。全てのユーザーはなおも独自のキーを選ぶことができ、自らのプ

ライベートキーを秘密理に保つことができる。それでも、法律により考慮されている適切な状況の下で（例えば裁判所命令）、これらの状況の下でのみ、特殊な承認済み加入者（例えば政府）、そしてこの加入者のみが、特定のユーザーに送られた全てのメッセージを監視することを許可される。公正なＰＫＣは、受入れられている合法的手続きの制約内にとどまりながら、既存の通信システム

（例えば電話業務）の機密保護を改善する。

一実施態様では、公正なＰＫＣは、以下の一般的方法で講成される。ここで図１～２を参照すると、５人の受託者２２ａ･･･２２ｃが存在し、裁判所命令を受けた時点で政府が発呼局１２へ又はこの発呼局からの電話通信を監視することを望んでいる、という仮定がなされている。上述の説明は特定的なものであるが、通信システムのユーザー及び受託者が人間であつてもよいし又は計算装置であつてもよいということがわかるはずである。受託者は、信頼のおける者となるよう選択されることが好ましい。例えば、受託者は、判事（又は判事が制御するコンピュータ）であつてもよいし、この目的のために特別に設置されたコンピュータであつてもよい。受託者は個々のユーザーと共に、システム内でどの暗号化キーが公表されるかを決定する上で重要な役目を果たす。

各各のユーザーは、一定の与えられたダブルキーシステムに従って自分自身のパブリックキー及びシクレットキーを選ぶ（例えば、パブリックキーは２つの素数の積から成り、シクレットキーはこれら２つの素数のうちの一方から成る）。ユーザーはそのキーの両方を選んでいるため、その「質」及び自らの暗号解読キーのプライバシーについて確信できる。このとき、ユーザーは自らのシクレット解説キーを、次の特性をもつ５つの特殊な「断片」（ｐｉｅｃｅ）に分割する（すなわち、彼は自らの暗号解説キーから５つの特別なストリング／番号を

計算する）。

（１）５つの特殊な断片が全てわかつている場合、プライベートキーを再構成できる。

（２）特殊な断片のうちいずれか４つ又はそれ未満しかわからない場合、プライ

ベートキーを推測することは全く不可能である。

（3）i－1，･･･5，については、i番目の特殊断片を個別に正しいものであると確認することができる。

5つの特殊な断片つまり「分担分」が与えられている場合、それらが実際にプライベート解読キーを生み出すことをチェックすることによりそれらが正しいことを確認することができる。本発明の1つの特徴に従うと、特性（3）は、個別に、すなわちシクレットキーを全く知らずに又その他の特殊な断片のいずれかの値を知ることなく、各各の特殊な断片を正しいものと（すなわちその他の4つの特殊断片と合わせてそれがプライベートキーを生み出すものであると）確認しうるということを保証している。

このとき、ユーザーはひそかに（例えば暗号化された形で）受託者22に対し独自のパブリックキー及びそれに結びついたシクレットキーのi番目の断片を与える。各各の受託者22は、自ら受けとつた断片を個別に検査し、それが正しい場合パブリックキーを承認し（それに署名する）、それに関連する断片を安全に保管する。これらの承認は、受託者によつて直接、又は受託者からそ

れらを収集する個々のユーザーにより（できれば単一のメッセージ内で）、キー管理センター24に与えられる。政府と一致している場合もあるしそうでない場合もあるセンター24は、それ自体、全ての受託者により承認されているあらゆるパブリックキーを承認（例えば署名する。これらのセンター承認キーは、公正なＰＫＣのパブリックキーであり、通常のＰＫＣの場合と同様に分配され、秘密通信のために用いられる。

各各の暗号解読キーの特殊な断片は受託者にひそかに与えられることから、2人のユーザーの通信回線を傍受する敵は、基礎を成す通常のＰＫＣ内と同じ情報を有する。かくして基礎をなすＰＫＣが機密保護性のあるものであるならば、公正なＰＫＣもかくの通りである。その上、敵が受託者自身の一人である場合、さらには受託者5人のうちのいずれか4人の協力する集まりであつた場合でも、特性（2）は、その敵がなお通常のＰＫＣの場合と同じ情報しか有さないことを保証する。敵が5人の判事のうちの5人を買収する可能性は絶対的に遠いものであ

ることから、結果として得られる公正なＰＫＣの機密保護性は、基礎を成すＰＫＣの場合と同じである。

例えば裁判所命令などが提示された時点で、受託者２２は政府２０に対して、自らが所有する一定の与えられた暗号解読キーの断片を暴露する。本発明に従うと、受託者は、この一定の与えられた暗号解読キーを所有するユーザーのアイデンティティに気付いていてもいなくて

もよい。こうして、そのユーザーの解読キーの分担分に対する要請をひとたび受託者が受理した時点で本来ならば、被疑者ユーザーを内報するかもしれない「危機にさらされた」受託者に対する付加的な安全性が提供される。

分担分を受理した時点で、政府は、与えられた暗号解読キーを再構成する。特性（３）により、各各の受託者は、一定の与えられた暗号解読キーの正しい特殊断片が自らに与えられたか否かを予め確認した。さらに全てのパブリックキーは、それが全ての受託者２２により承認された場合に初めてキー管理センター２４により許可された。従って、政府は、裁判所命令の場合、あらゆる暗号解読キーの全ての特殊断片を与えられるという保証を得る。特性（１）により、これは、政府が必要とあらば回線網全体にわたる通信を監視するためあらゆる与えられた解読キーを再構成できるようになるという保証である。

公正なＰＫＣのいくつかのタイプについて、以下でさらに詳細に説明する。

Ｄｉｆｆｉｅ及びＨｅｌｌｍａｎのＰＫＣ

Ｄｉｆｆｉｅ及びＨｅｌｌｍａｎのパブリックキー暗号システムは既知のものであり、本発明により公正なＰＫＣへと容易に変換される。Ｄｉｆｆｉｅ及びＨｅｌｌｍａｎのスキーム（ｓｃｈｅｍｅ）においては、各各のユーザー対Ｘ及びＹは、いかなる対話もなく、従来のシングルキー暗号システムとして使用されるべき共通のシ

クレットキーＳｘｙについて合意するのに成功する。普通のＤｉｆｆｉｅ－Ｈｅｌｌｍａｎ　ＰＫＣでは、全てのユーザーに共通の素数Ｐと生成元（又は高位元）ｇが存在する。ユーザーＸは、自らのプライベートキーとして間隔［１，ｐ－

1］で無作為整数Ｓｘを秘密理に選択し、自らのパブリックキーとして、Ｐを法として整数Ｐｘ＝ｇSxを公表する。もう一人のユーザーＹは、自らのプライベートキーとして同様にＳｘを選択し、自らのパブリックキーとしてＰを法としてＰｙ＝ｇSyを公表する。このキーの値は、Ｐを法としてＳｘｙ＝ｇSxSyとして決定される。ユーザーＸは、Ｙのパブリックキーを ＰＸを法として自らのプライベートキーまで上げることにより、又ユーザーＹはＸのパブリックキーをＰを法として自らのシクレットキーまでもち上げることによつて、Ｓｘｙを計算する。実際：Ｐを法として（ｇSx）Sy＝ｇSxSy＝Ｓｘｙ＝ｇSxSy＝（ｇSy）Sxである。

ｇ，ｐ及びｘがわかつている場合、ｐを法としてｙ＝ｇxを計算するのは容易であるが、一方、ｇが充分に高い位数を有する場合、ｙ及びｐがわかつていて、ｐを法としてｇx＝ｙとなるようなｘを計算するのに効率のよいアルコリズムは全く知られていない。これは、離散的な対数の問題である。この問題は、多くの暗号システムにおいて機密保護のベースとして用いられてきた。Ｄｉｆｆｉｅ及びＨｅｌｌｍａｎのＰＫＳはは、以下の要領で公正なものへと変換される。

各ユーザーｘが無作為に間隔［１，ｐ－１］で５つの整数Ｓｘ１，…Ｓ×５を選択しＳｘをｐを法としたその和にする。以下の全ての演算がｐを法としたものであると理解すべきである。このとき、ユーザーｘは、次の数を計算する：

ｔ１＝ｇS×l，…ｔ５＝ｇS×5及びＰｘ＝ｇSx　。

Ｐｘはユーザーｘのパブリックキーであり、Ｓはそのプライベートキーである。ｔｉは、Ｐｘのパブリック断片として参照され、Ｓｘｉはプライベート断片として参照される。又パブリック断片の積がパブリックキーＰｘに等しいことに留意すべきである。実際：

ｔ１…ｔ5＝ｇS×l，…ｇS×5＝ｇ(S×l＋…＋S×5)＝ｇSx

Ｔ１，…Ｔ５を５人を受託者とする。このときユーザーｘはＰｘ，パブリック断片及びＳｘ１を受託者Ｔ１に与え、Ｐｘ，パブリック断片及びＳｘ２を受託者Ｔ２にたいし与え、以下同様に続く。断片Ｓｘｉは受託者Ｔｉに対し秘密に与えられる。パブリック及びプライベート断片ｔｉ及びＳｘｉを受理した時点で、受託者ＴｉはｇSxi＝Ｔｉであるか否かを確認する。そうである場合、受託者は対

（Ｐｘ，Ｓｘｉ）を保存し、数列（ｐｘ，ｔ１，ｔ２，ｔ３，ｔ４，ｔ５）に署名し、署名した数列をキー管理センター２４（又は、その後署名したパブリック断片全てを一度にキー管理センターに与えることになるユーザーｘ）に与える。一定の与えられたパブリッ

クキーＰｘに関する署名された数列全てを受理した時点で、キー管理センターは、これらの数列がパブリック断片ｔ１･･･ｔ５の同じ部分列を含むこと、そしてパブリック断片の積が実際にＰｘに等しいことを確認する。そうである場合、センター２４はＰｘをパブリックキーとして承認し、それをもとのスキームの場合と同様に分配する（例えばそれに署名し、ユーザーｘにそれを与える）。ユーザーｘ及びｙのいずれの対についての暗号化及び暗号解読の指令も、Ｄｉｆｆｉｅ及びＨｅｌｌｍａｎのスキームの場合と正に同じである（すなわち共通のシクレットキーＳｘｙを用いる）。

この手順は、公正なＰＫＣを構成する前述の方法と符合する。Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎのスキームのさらにもう１つの公正なバージョンは、ユーザーに各各の受託者Ｔｉに対してパブリック断片ｔｉとそれに相応するプライベート断片Ｓｘｉのみを与えさせ、ユーザーにキー管理センターに対しパブリックキーＰｘを与えさせることによつて、より単純な要領で得ることができる。センターは、それが適切な受託者により署名された全てのパブリック断片を受理しこれらのパブリック断片の積がＰｘに等しい場合にのみ、Ｐｘを承認することになる。このようにして、受託者Ｔｉは、Ｓｘｉがパブリック断片ｔｉの離散的対数であることを確認することができる。このような受託者は、Ｐｘ又はその他のパブリック断片を見たことがないため、ＳｘｉがＰｘの合法的分担分で

あることを確かに確認することができない。それでもなお、上述の特性（１）－（３）がなおも満たされていることから、結果はＤｉｆｆｉｅ－Ｈｅｌｌｍａｎのスキームに基づく公正なＰＫＣである。

上述の公正なＰＫＣのうちいずれのものも、基礎をなすＤｉｆｆｉｅ－Ｈｅｌｌｍａｎのスキームにより提供されるものと同じレベルの通信のプライバシーを

有する。実際、パブリックキーの妥当性検査は相応するプライベートキーを危機にさらすことがない。各各の受託者Ｔｉは、特殊な断片として、無作為数ｔｉの離散的対数Ｓｘｉを受理する。この情報は明らかに、Ｐｘの離散的対数を計算する不適切なｆｒである。いずれの４つの特殊断片もプライベート暗号キーＳｘとは独立したものであることから、受託者のうちいずれか４人を合わせて考えた場合にも、実際、同じことが言える。同様にキー管理センターは、Ｐｘの離散的対数という、プライベートキーに関するいかなる情報も有していない。センターが有しているのは、受託者によりそれぞれ署名されたパブリック断片だけである。パブリック断片は、その積がＰｘである５つの無作為数にすぎない。このタイプの情報は、Ｐｘの離散的対数を計算するのに不適切である。実際、誰でも４つの整数を選び、５つ目を、最初の４つの積でＰｘを除したものとして設定することができる。除算がｐを法とするものであることから、結果は整数となる。受託者の署名については、これは、他の誰かがシクレッ

ト断片を有するという裏付けを表わすにすぎない。

いずれか４人の受託者と合わせたセンターの手中にある情報でさえ、プライベートキーＳｘを計算するのに不適切である。従って、ユーザーは、妥協性検査手順が自らのプライベートキーを密告しないという保証を得るのみならず、自分自身のキー及び自らのプライベートキーの断片を計算するのが彼自身であることから、この手順が適切に追従されたこともわかるのである。

第２に、キー管理センターがパブリックキーＰｘを妥当性検査した場合、そのプライベートキーは、裁判所命令の場合に政府により再構成可能なものとして保証される。実際、センターは、各各適切な受託者により署名されたＰｘの５つの断片すべてを受理する。これらの署名は、受託者Ｔｉがパブリック断片ｔｉの離散的対数を有することを保証する。センターは、パブリック断片の積がＰｘに等しいことを確認するため、受託者と共に保管中のシクレット断片の和がＰｘの離散的対数すなわちユーザーｘのプライベートキーに等しいということも知っている。従って、センターは、ｘのプライベートキーを要求する裁判所命令が発行された場合、政府は受託者が受理した値を合計することによつて必要とされるプラ

イベートキーが得られるという保証を受けているということを知っている。

ＲＳＡの公正なＰＫＣ：

以下では、既知のＲＳＡ関数に基づく公正なＰＫＣを

記述する。通常のＲＳＡＰＫＣでは、パブリックキーは２つの素数と１つの指数ｅ（Ｆをｔそう－の商関数としてｆ（Ｎ）と互いに素なもの）の積である整数Ｎから成る。指数の如何に関わらず、プライベートキーはつねにＮの因数分解となるように選択されうる。簡単な背景として示すと、ＲＳＡスキームは以下のような数論的様相から派生するいくつかの特徴を有する：

事実１．Ｚｎ*が１～Ｎの間にありＮと互いに素な整数の乗法群を示すものとする。Ｎが２つの素数の積であるつまりＮ＝ｐｑ（又は２つの素数べき；Ｎ＝ｐａｐｂ）であるならば、そのとき、

（１）Ｚｎ*中の数字ｓは、それがＮを法として４つの全く異なる平方根すなわちｘ，Ｎを法として－ｘ，ｙ及びＮを法として－ｙを有する場合（すなわちｘ２＝ｙ２＝Ｎを法とするｓ）にのみ、Ｎを法として平方数である。さらに＋　－ｘ　＋　－ｙ及びＮの最大公約数からＮの因数分解が容易に計算される。同様に：

（２）Ｚｎ*内の数のうち４つの中の１つは、Ｎを法として平方数である。

事実２．Ｚｎ*中の整数の間で、１又は－１のいずれかに容易に評価するヤコビの記号という１つの関数が定義づけられる。ｘというヤコビの記号は乗法的である。すなわち（ｘ／Ｎ）（Ｙ／Ｎ）＝（ｘｙ／Ｎ）。Ｎが２つの素数の積Ｎ＝ｐｑ（又は２つの素数べき：Ｎ＝ｐａｐｂ）であるならば、ｐ及び１は、４を法として３に対

し合同である。このとき＋　－ｘ及び＋　－ｙがＮを法とした平方の４つの平方根である場合、（ｓ／Ｎ）＝（－ｘ／Ｎ）＝＋１であり（ｙ／Ｎ）＝（－ｙ／Ｎ）＝－１である。かくして、事実１から、あらゆる平方のヤコビの記号１ルート及びヤコビの記号－１ルートが与えられている場合、Ｎを容易に因数分解できる。

この背景から、以下では、ＲＳＡ暗号システムをいかにして単純に公正なもの

にすることができるかについて記述する。単純化を期して、ここでも又５人の受託者が存在し、そのうちのいずれの４人もシクレットキーを予想さえできないのに、この１つのシクレットキーを再構成するためにはこれら５人全員が協力しなければならない、という仮定をする。ＲＡＳ暗号システムは、受託者とＮの因数分解を効果的に共有することにより、公正なＰＫＣへと容易に変換される。特に、受託者は、おそらくしその他の与えられた共通の情報と合わせて、Ｎを法として共通の平方の２つ（又はそれ以上）の平方根ｘ及びｙ（ｘはＮを法として±ｙと異なる）を再構成できるようにする情報の提供を秘密に受けている。与えられた共通の情報は、ｙに等しいｘ2の－１のヤコビの記号のルートであつてよい。

ユーザーが自らのプライベートキーとして４を法として３に合同なＰ及びＱの素数を、又そのパブリックキーとしてＮ＝ＰＱを選ぶ。次に彼は、Z_{N}^{*}の中で５つのヤコビ１整数x_1，x_2，x_3，x_4及びx_5（好ましくは無作為に）を選び、全てのｉ＝１，･･･，５についてＮを法としてその積ｘ及びｘｉ2を計算する。最後の５つの平方の積Ｚはそれ自体平方である。Ｎを法としてＺの１平方根はｘであり、これは１に等しいヤコビの記号をもつ（ヤコビの記号は乗法的であるため）。ユーザーは、Ｎを法としてヤコビ－１ルートの１つであるＹを計算する。x_1，･･･x_5はパブリックキーＮのパブリック断片となり、ｘｉはプライベート断片となる。ユーザーは受託者にプライベート断片ｘｉ（そして場合によつては、特性（１）－（３）を満たすべく分担分の確認が受託者とセンターの両方によつて行なわれるか受託者により単独で行なわれるかによつて、相応するパブリック断片、その他全てのパブリック断片及びＰｘ）を与える。受託者Ｔｉは、Ｎを法としてｘｉを２乗し、キー管理センターに自らのx_1^2の署名を与え、ｘｉを保管する。

センターはまず、（－１／Ｎ）＝１であることすなわち全てのｘについて（ｘ／Ｎ）＝（－ｘ／Ｎ）であることをチェックする。Ｎのパブリック断片の有効な署名及びヤコビ－１の値Ｙをユーザーから受理した時点で、センターは、Ｎを法としてＹの平方が５つのパブリック断片の積に等しいか否かチェックする。等しい場合、センターは、できればユーザーの助けをかりてＮが２つの素数べきの積

であることをチェックする。そうである場合、センターはNを承認する。

このスキームの背後にある論法は以下のとおりである。

すなわち、ｘｉ2の（Nを法として）受託者の署名は、全ての受託者ＴｉがNを法としてｘｉ2ののヤコビの記号１のルートを保管したことを保証する。かくして、裁判所命令があつた場合、これらのヤコビの記号１のルート全てが研削可能である。Nを法としてそれらの積は、この関数が乗法的であることから、同様にヤコビの記号１を有することになり、Nを法としてｘ2のルートとなる。しかしセンターがNを法としてｙ2＝ｘ2であることを確認したことから、Nを法として共通平方の２つのルートｘ及びＹを有することになる。その上、Ｙは、異なるヤコビの記号を有することからｘとは異なり、又（－１／N）が１つであることがチェックされ（ｂ）ヤコビの記号が乗法的であるため（－ｘ／N）＝（ｓ／N）であることから、－ｘとも異なっている。事実１及び２により、このような平方根を有することは、Nがせいぜい２つの素数ベキの積であることを条件としてNの因数分解を有することを同等である。この最後の特性は同様に、センターがNを承認する前にチェックしていたものである。

Nがせいぜい２つの素数ベキの積であるとの確認はさまざまな方法で実行できる。例えば、センターとユーザーは、この事実のゼロ－知識の証明に携わることができる。代替的には、ユーザーはセンターに、整数の規定された及び充分に無作為の数列の形で整数のおよそ１／４についてNを法として平方根を提供することができる。

例えば、このような数列は、短いシードへNを一方向に切り刻み次に偽似無作為な生成之を用いてより長い数列へとそれを拡張させることによつて決定できる。不正直なユーザーが自らのNを３つ以上の素数べきの積であるように選択した場合、彼がその数列内の整数の約１／４がNを法とした平方であることを望むのはバカげたことである。実際、このユーザーのNという選択に対しては、整数のせいぜい１／８がNを法として平方根をもつ。

<u>変形態様</u>

上述のスキームは数多くの方法で修正することができる。例えば、Nが２つの素数べきの積であることの証明を受託者が（ユーザーと協力して）行なうことができ、この受託者は次にその発見事実についてセンターに情報を提供する。同様に、いずれかの少数者がシクレットキーに関する情報を得ることができなくなつても、シクレットキーを再構成するには受託者の大部分の協力があれば充分であるように、スキームを修正することもできる。同様に、全ての公正な暗号システムの場合のように、政府が１人の受託者に対して、同者が所有するユーザーシクレットキーの断片を要求したときにこの受託者がそのユーザーのアイデンティティについて学習しないように配慮することもできる。これらの変形態様について、以下でさらに詳細に論述する。

特に、上述のスキームは、偶然にであれ悪意をもつてであれ幾人かの受託者がシステムの機密保護を危険にさ

らすことなく自ら所有する分担分を暴露しうるという意味で、頑丈なものである。しかしながらこれらのスキームは、受託者が再構成段階中協力し合うという事実に依存している。実際、シクレットキーを回復させるためには全ての分担分が必要でなくてはならない、という点が強調された。この必要条件は、幾人かの受託者が信頼に値しないことがわかつたり又は自ら所有するキーを政府に与えるのを拒絶する可能性があること、又は全てのファイルバックアップにも関わらず受託者が自ら所有する情報を純粋に紛失してしまう可能性があることのいずれかを理由として、不利なものでありうる。その理由の如何に関わらず、この状況下ではシクレットキーの再構成は妨げられることになる。この問題も又、本発明によつて解決される。

背景として、「秘密共有」（パラメータｎ，Ｔ，ｔでの）は、次の２つの段階から成る先行暗号スキームである。すなわち第１段階では、卓越した人物つまりディーラーにより選ばれたシクレット値が、ｎ人又はｎ個の人物又はコンピュータつまり受託者の各各に１つの情報断片を与えることにより、これらの受託者に安全に保管される。第２段階では、受託者が情報を自らの所有下にまとめてプールした時点で、シクレットが回復される。秘密共有は、主要な１つの欠点を有す

る。すなわちここでは、ディーラーが自らのシクレット値についての正しい分担分（情報断片）を受託者に与える、ということを前

提としているのである。「確認可能な秘密共有」（ＶＳＳ）はこの「正直さ」の問題を解決する。ＶＳＳスキームでは、各各の受託者は、そのシクレット（秘密）自体のその他の受託者の分担分を全く知ることなく、自らに与えられた分担分が本物であることを確認することができる。特定的に言うと、受託者は、Ｔ個の確認された分担分が暴露された場合、もとのシクレットは、ディーラー又は不正直な受託者が何をしようと再構成されることになる、ということを確認することができる。

上述の公正なＰＫＣスキームは、パラメータｎ＝５，Ｔ＝５及びｔ＝４で、適正に組織化された非対話型の確認可能な秘密共有スキームに基づいている。本発明に従うと、これらのパラメータの異なる値、例えばｎ＝５，Ｔ＝３及びｔ＝２を有することが望ましい可能性がある。このような場合、少数の受託者の誰も全くシクレットキーを予測できないのに対して、いずれかの大多数の受託者がこれを回復させることができる。これは以下のとおり達成される（そしてＴ＞ｔである望ましいｎ，Ｔ及びｔのあらゆる値まで単純に一般化される）。

Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎスキームのためのサブセット方法

［１，ｐ－１］内でシクレットキーＳｘを選択した後、ユーザーｘは、ｐを法として自らのパブリックキーＰｘ＝ｇSXを計算する（以下の計算は全てｐを法とする）。ユーザーｘは次に１と５の間の数の全ての三ツ組すなわ

ち（１，２，３），（２，３，４）などを考慮する。各三ツ組（ａ，ｂ，ｃ）について、ユーザーｘは、そのｐを法とした和がＳｘに等しくなるように間隔［１，ｐ－１］内で３つの整数Ｓ１ａｂｃ，…，Ｓ３ａｂｃを無作為に選ぶ。その後ユーザーｘは、次の数を計算する：

ｔ１ａｂｃ＝ｇS1abc，ｔ２ａｂｃ＝ｇS2abc，ｔ３ａｂｃ＝ｇS3abc

ｔｉａｂｃはＰｘのパブリック断片とＳｉａｂｃはプライベート断片と呼ばれることになる。ここでも又、パブリック断片の積はパブリックキーＰｘに等しい

。実際、

ｔ１ａｂｃ･･･ｔ２ａｂｃ･･･ｔ３ａｂｃ＝ｇS1abc･gS2abc･gS3abcｘ＝ｇ（S1aab＋･･･＋S3ab）＝ｇSx＝Ｐｘ

ユーザーｘは次に受託者Ｔａにｔ１ａｂｃ及びＳ１ａｂｃ、受託者Ｔｂにｔ２ａｂｃ及びＳ２ａｂｃ及び受託者Ｔｃにｔ３ａｂｃ及びＳ３ａｂｃを与え、つねに問題の三ツ組を規定する。これらの数量を受理した時点で、受託者Ｔａ（その他の全ての受託者も何か類似のことをする）は、ｔ１ａｂｃ＝ｇS1abcであることを確認し、値［Ｐｘ，ｔ１ａｂｃ，（ａ，ｂ，ｃ）］を署名し、署名を管理センターに与える。

キー管理センターは、各各の三ツ組（ａ，ｂ，ｃ）について、受託者Ｔａ，Ｔｂ及びＴｃから受理した署名された情報から値ｔ１ａｂｃ，ｔ２ａｂｃ及びｔ３ａｂｃを検索する。これら３つの値の積がＰｘに等しく、署名

が有効である場合、センターはＰｘをパブリックキーとして承認する。

多くても２人の受託者が信頼に値しないということを仮定して、このスキームが有効である理由は、１つのシクレットキーを計算する（又は予測する）ために１つの３つ組の全てのシクレット断片が必要とされる、ということにある。従って、システム内のいずれのシクレットキーもいずれか２人の受託者によつて検索され得ない。一方、裁判所命令の後では、少なくとも３人の受託者が、一定の与えられたパブリックキーについての自らの所有する全てのシクレット断片を暴露する。このとき政府は、少なくとも１つの三ツ組について必要なシクレット断片全てを有し、かくして望まれるシクレットキーを容易に計算することができる。

代替的には、各各の受託者は一群の新しい受託者によつて置換される。例えば、単一の受託者Ｔａの代わりに３人の受託者つまりＴａ１，Ｔａ２及びＴａ３が存在する可能性がある。これらの受託者の各各は、受託者Ｔａの同じ分担分を受理し、これをチェックすることになる。このようにして、３人の受託者全てが第１の分担分の自らのコピーを引き渡すことを拒絶する確率は非常に低い。

悪意をもつ可能性のある数人の受託者がキーの再構成を妨げることはできないということを確信した後、さらにもう１つここでとり上げるべき安全性の問題が

ある。すなわち、（一定の与えられたシクレットキーの自らの

分担分を引渡すよう裁判所命令により要請された）受託者はそのキーの所有者に対し自らの通信が監視されようとしているという警告を行なうことができるのである。この問題も又本発明により解決される。受託者が使用する暗号システムがいくつかの代数的特性を有する場合、１つの単純な解決法がもち上がる。このことを、ＲＳＡスキームについても同じ結果が起こるものの、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎのケースについて例示しておく。以下の論述においては、単純化のため、全ての受託者がシクレットキーの再構成において協力し合うということを仮定している。

気付かれるかつ公正なＤｉｆｆｉｅ－Ｈｅｌｌｍａｎのスキーム

全ての受託者が、秘密のメッセージを受理するのに決定論的ＲＳＡを使用すると仮定する。かくして、Ｎｉを受託者Ｔｉのパブリックモジュラスとし、ｅｉを彼の暗号化指数とする（すなわちＴｉに暗号化された形のメッセージmを送るためには、Ｎｉを法としてmeiを送ることになる）。

ユーザーＵは、それぞれＰｘ及びＳｘという自らのパブリックキーとシクレットキー（従ってＰを法としてＰｘ＝ｇSx）ならびにそれぞれｔｉ及びＳｘｉというシクレットキーの自らのパブリック断片とシクレット断片（従ってＰを法としてＰｘ＝ｔ１，ｔ２･･･ｔ５及び全てのｉについてＰを法としてｔｉ＝ｇSxi）を準備する。

その後ユーザーはキー管理センターに対して、Ｐｘ全てのｔｉ及びｎ値、Ｎｉを法としてＵｉ＝（Ｓｘｉ）3、を与える；すなわち、ユーザーは受託者Ｔｉのパブリックキーでｉ番目の分担分を暗号化する。センターはＮｉの因数分解を知らないため、これは、Ｓｘを予測するのに有用な情報ではなく、又センターは、ｎ個の暗号文の解読がＳｘの適切な分担分であることを確認することができない。このため、センターは、ｎ人の受託者の協力を求めるが、以下に記すように彼らに対しユーザーのアイデンティティについての情報は提供しない。

センターは、ユーザーＵに関して値ｔｊ及びＵｊを保管し、次にＵｉ及びｔｉ

を受託者Ｔｉへと転送する。全ての受託者Ｔｉが、Ｕｉの暗号解読がｔｉに関する適切なプライベート断片であることを確認した場合、センターはＰｘを承認する。

ここで、司法当局がユーザーUの通信を監視する決定を下すと仮定する。疑いのあるユーザーのアイデンティティを受託者に洩らすことなくシクレットキーＳｘを合法的に再構成するため、判事（又はもう１つの認可された代理人）は、Ｎｉを法として数Ｒｉを無作為に選択し、Ｎｉを法としてｙｉ＝Ｒｉeiを計算する。このとき、彼は受託者Ｔｉに対してＮｉを法として値Ｚｉ＝Ｕｉ－ｙｉを送り、裁判所命令をもつてｗｉ、つまりＮｉを法としたＺｉのｅｉ番目のルートを計算し送り返すよう依頼する。Ｕｉの値の如何に関わらず、ＺｉはＮｉを法とした無作為な数であることから、受託人Ｔｉは問題のユーザーUのアイデンティティを推測することができない。その上、ＺｉはＮｉを法としてＵｉ及びｙｉの積であることから、Ｚｉのｅｉ番目のルートは、Ｕｉのｅｉ番目のルート（すなわちＳｘｉ）とｙｉのｅｉ番目のルート（すなわちＲｉ）のＮｉを法とした積である。従って、ｗｉを受理した時点で、判事はそれをＮｉを法としたｙｉで除し、かくして望ましいＳｘｉを計算する。これらのＳｋｉの積は望ましいＳｘに等しい。

さらなる変形態様

本発明のその他の変形態様においては、裁判所命令があつた場合、政府は、制限された量の時間について一定の与えられたユーザーに関するメッセージを理解することだけが許される。全ての受託者の共同の承認は、政府の承認に代わりうる。同様に、受託者は、プライベートキーの自らの断片を保管する必要がない。（受託者のパブリックキーの中にあり受託者により署名された）この断片の暗号化を、ユーザーのパブリックキーの一部とすることもできる。このようにして、パブリックキーはそれ自体の真正性及び確認の証明を有している。後者の場合、受託者のプライベートキーを断片に分割することが有利でありうる。

ユーザーが集積回路チップといつた電子デバイスである場合、キー選択及びパブリックキーの妥当性検査の基本的プロセスは、デバイスが工場を離れる前に行

なうこ

とができる。この場合、受託者の「コピー」を工場内に維持できることが有利であるかもしれない。受託者のコピーは、受託者の暗号解読キーのコピーを含む物理的に安全なチップ（そのデータが読み取り不可能なもの）である。受託者（すなわち裁判所命令に基づいてプライベートキーの断片を与えることのできる当事者）は必ずしもこのデバイスと一致する必要はない。

もう１つの変形態様においては、受託者の各各が政府のプライベートキーの１断片を有し、各各のユーザーのプライベートキーが政府のパブリックキーを伴って暗号化されるように配慮することができる。

電気通信回路網内（そして政府の権力下での）公正なＰＫＣの使用について記述されてきたが、このような記述は、制限条件として考えられるべきものではない。公正なＰＫＣは、私的組織内でも使用できる。例えば、プライバシーに対するニーズがある大きい組織において、確立した「上司」が存在するものの、従業員があまりにも多すぎるため全ての従業員が信頼できるわけではないと仮定する。プライバシーに対するニーズのため、暗号化の使用が必要となる。全ての従業員が信頼できるわけではないため、全社的に単一の暗号化キーを使用することは、一定数のシングルキー暗号システムを使用すること（これは莫大なキー分配の問題を生みだすため）と同様に、受入れることのできないことである。各各の従業員に独自のダブルキーシステムを使用させることも又、

極秘裏に、無事にかつ便利に会社に対する陰謀を企てることができるようになるため、同様に危険である。

公正なＰＫＣのこのような利用分野においては、数多くの利点が得られる。まず第１に各各の従業員は、独自のキーの選択を担っている。より分配された手順の利点を享受する一方で、組織は、上司が必要とする場合に全ての従業員の通信を解読できるよう保証されていることから、絶対的な管理力を保持している。受託者を変更する必要がないことから、上司が変ってもキーを変える必要は全く無い。受託者の保管場所は、その全てを危険にさらすことのみが敵に何らかの利点

を与えることになるため、さほど監視を必要としない。

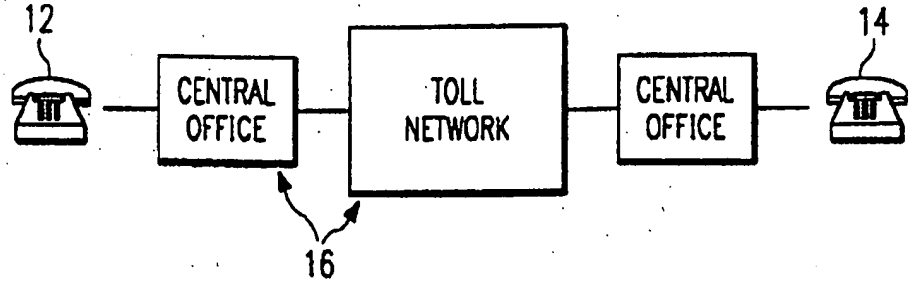
プライベートキー暗号システムを公正なものとするためだけではなくＰＫＣのためにも、各各の受託者がまず最初に、自ら分担分の暗号化されたバージョン又はその他の形で掛り合ったバージョンを寄託し、かくして自らの分担分が何であるかを暴露するよう依頼されたとき、その値について心変わりできないようにしておくことが望ましい。同様に、ユーザーが、署名した状態で受託者に自らの分担分を与えることが望ましい。このような署名は異なるパブリックキー（それらがデジタル式の署名である場合）に関するものであつてもよいし、又は署名にも新しいキーを用いることができる場合には同じ新しいパブリックキーに関するものであつてもよい。このようにして、受託者により暴露された分担分は、明らかに

それが創作されたものであることを証明する。なお良いことに、ユーザーは、受託者に与えられた分担分の暗号化に（受託者のキーで）署名することができ、署名は分担分と合わせて暴露されうる。このアプローチにより、暴露されたものがユーザーにより承認された分担分であつたことと同様に、受託者とユーザーが後にその値を変更する上で協力できないことの両方について確信が得られる。

当業者であれば、以上で開示されている特定の実施態様が、本発明の同じ目的を実施するためのその他の技術及びプロセスを修正又は設計するための１つの基礎として容易に利用できるものであるということがわかるはずである。当業者ならば、このような同等な構成が添付のクレーム内に記載されているような本発明の精神及び範囲から逸脱するものでないということも認識できるはずである。

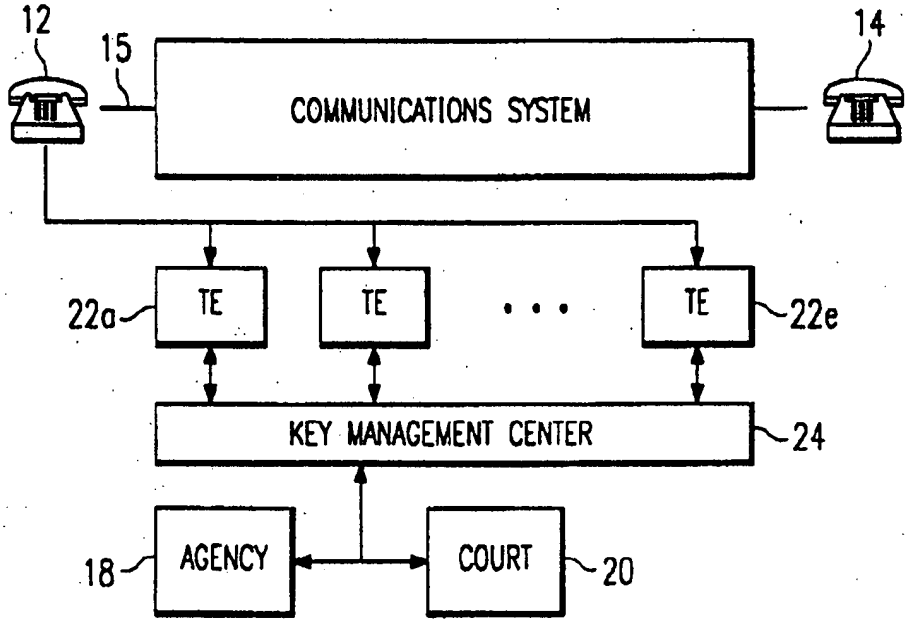
【図1】

FIG. 1



【図2】

FIG. 2



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US93/03666

A. CLASSIFICATION OF SUBJECT MATTER
IPC(5) :H04K 1/00
US CL :380/30
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 380/28,42-44

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US, A, 4,375,579 (DAVIDA ET AL.) 01 March 1983.	1-18
A	US, A, 4,933,970 (SHAMIR) 12 June 1990.	1-18
A	US, A, 5,006,200 (FISCHER) 02 April 1991.	1-18
A	US, A, 5,018,196 (TAKARAGI ET AL.) 21 May 1991.	1-18
A,P	US, A, 5,136,643 (FISCHER) 04 August 1992.	1-18
A,P	US, A, 5,150,411 (MAURER) 22 September 1992.	1-18

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be part of particular relevance
"E" earlier document published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 JUNE 1993	02 AUG 1993
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. NOT APPLICABLE	Authorized officer TODD SWANN Telephone No. (703) 308-0475

Form PCT/ISA/210 (second sheet)(July 1992)

【要約の続き】
ようなユーザーのシクレットキーの分担分を暴露する。こうしてエンティティ（18）はシクレットキーを再構成し、被疑者ユーザーの通信を監視することができるようになる。